FAULT TREE ANALYSIS (FTA)

DEFINITION FTA

- **A TOP-DOWN APPROACH TO FAILURE ANALYSIS STARTING WITH AN UNDESIRABLE EVENT CALLED A TOP EVENT, SUCH AS A FAILURE OR MALFUNCTION AND THEN DETERMINING ALL THE WAYS IT CAN HAPPEN**
- **The analysis proceeds by determining how these top events can be caused by individual or combined lower level failures or events.**

FTA USES

- **Fault-trees have been widely used to investigate the reliability and safety of complex and large systems for diagnostic applications.**
- **The main reason for the widespread use of fault-tree analysis (particularly in nuclear and aerospace industries is due to concern for human safety).**
- **If there is a critical failure mode, then all possible ways that mode could occur must be discovered.**
- **First used by Bell Telephone Laboratories in connection with the safety analysis of the Minuteman missile launch control system in 1962.**

OBJECTIVES:

- Be able to answer (or perform):
- What is the difference between an FTA and FMEA.
- When is each used?
- What are the key components of a FTA?
- How is each used?
- Be able to do a simple FTA.

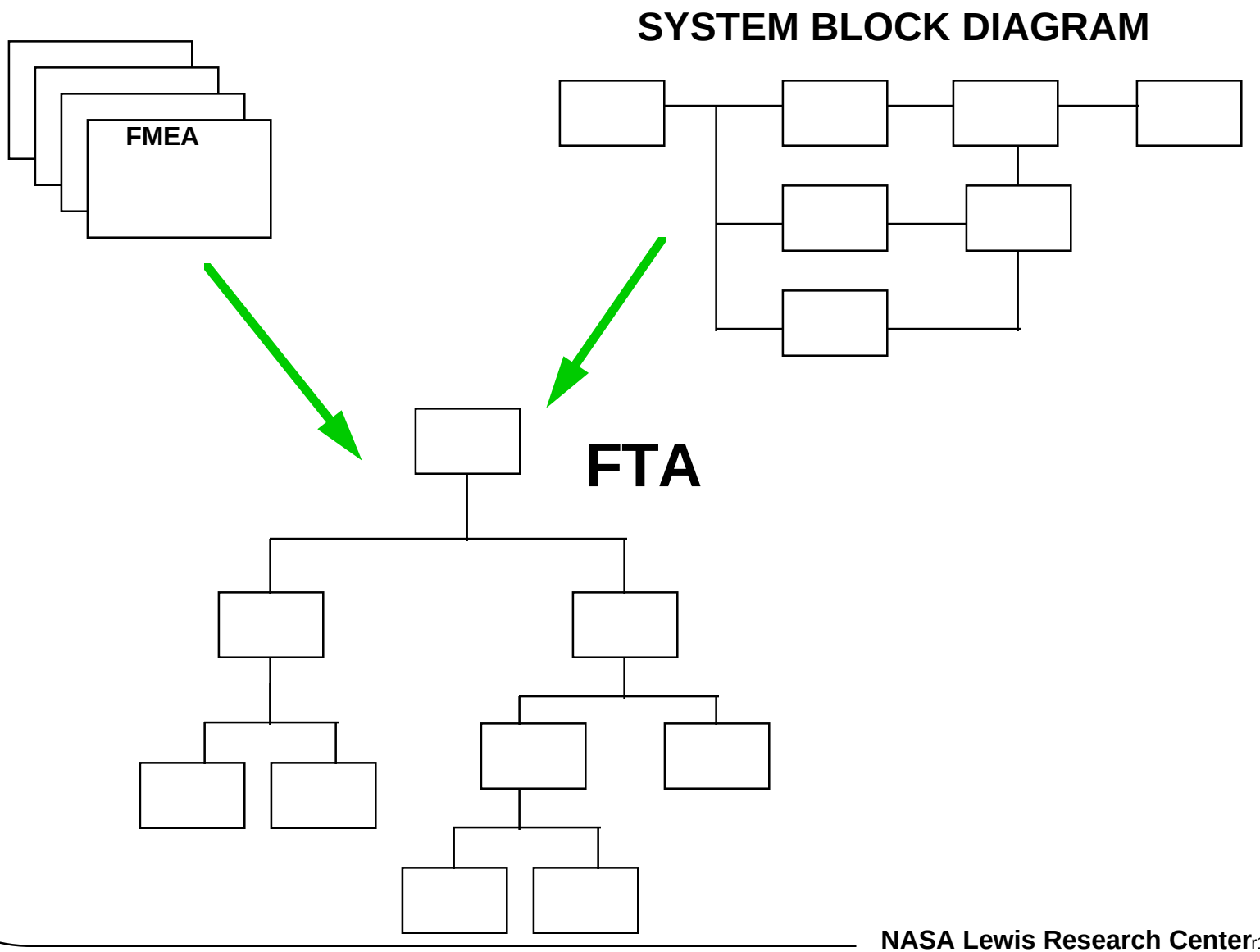
OUTLINE

- **Preparation of an FTA.**
- **Procedure for writing an FTA.**
- **Standard Symbols of an FTA.**
- **Sample Problems.**

Preparation for FTA

- First (usually) a FMEA is constructed as well as a [FMEA] system block diagram.
- The design, operation and environment of the system are evaluated.
- The cause and effect relationships leading to the failure of the system are identified.
- The FMEA is an essential first step in understanding the system.
- Also, a function or flow diagram for the processes of the system is constructed.

Preparation of a FTA



FTA Requirements

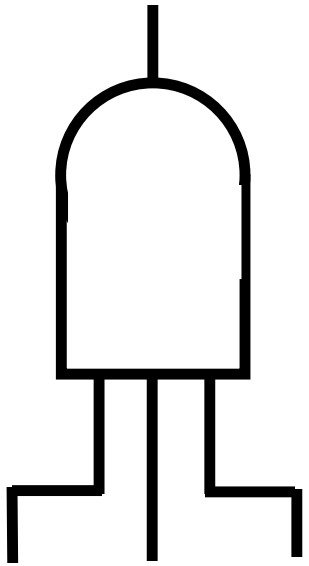
- Thorough knowledge of how the system works.
- Knowledge of the logic relationships in the system (interlocks, control interfaces, power supply feeds).
- Thorough knowledge of how the software works (evaluated separately).

FTA Procedure

- Identification of the top event(s) to be analyzed.
- Identify the events or series of events that directly contribute to the top level event.
- Continue this process until the lowest level defined or basic level is reached.
- The two basic symbols used are:
- AND gate: the output will be present only if ALL of the inputs are present.
- OR gate: the output will be present if one or more of the input events are present.

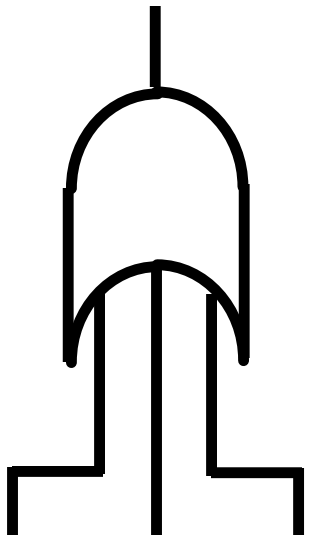
Standard Symbols for FTA Construction

AND GATE



Next level failure if ALL inputs fail.

OR GATE



Next level failure if ANY inputs fail.

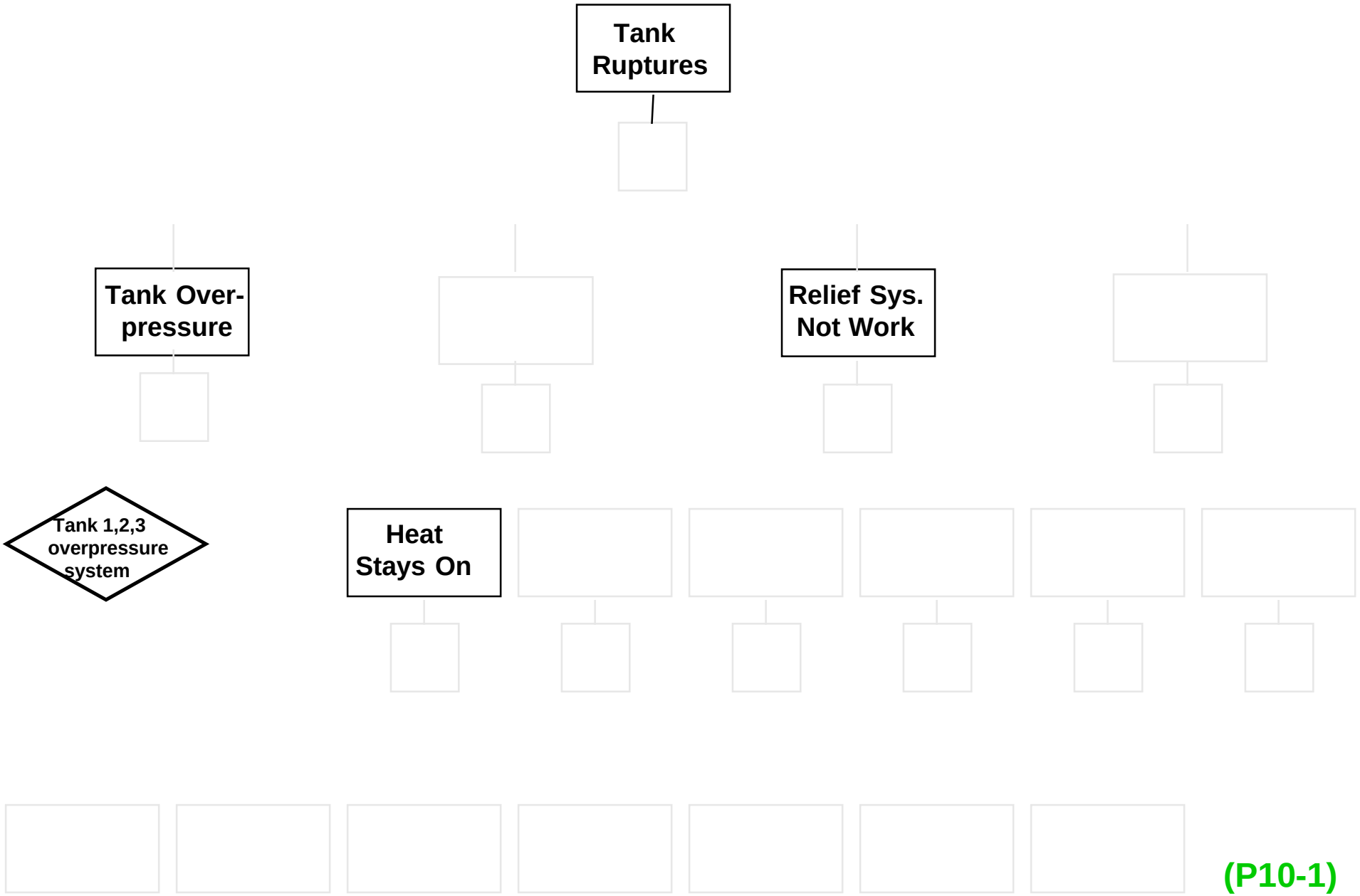
Table - FTA

Example 1 - Space Experiment Main Tank Overpressure.

- Consider the top level event (a single failure mode) of tank overpressure.
- Develop a FTA to discover all the events necessary for this event to occur.
- Are their any common mode failures?
- How can the system be improved?

F

FAULT TREE ANALYSIS of _____ by:___ Date __/__/__



CONCLUSION-FTAs

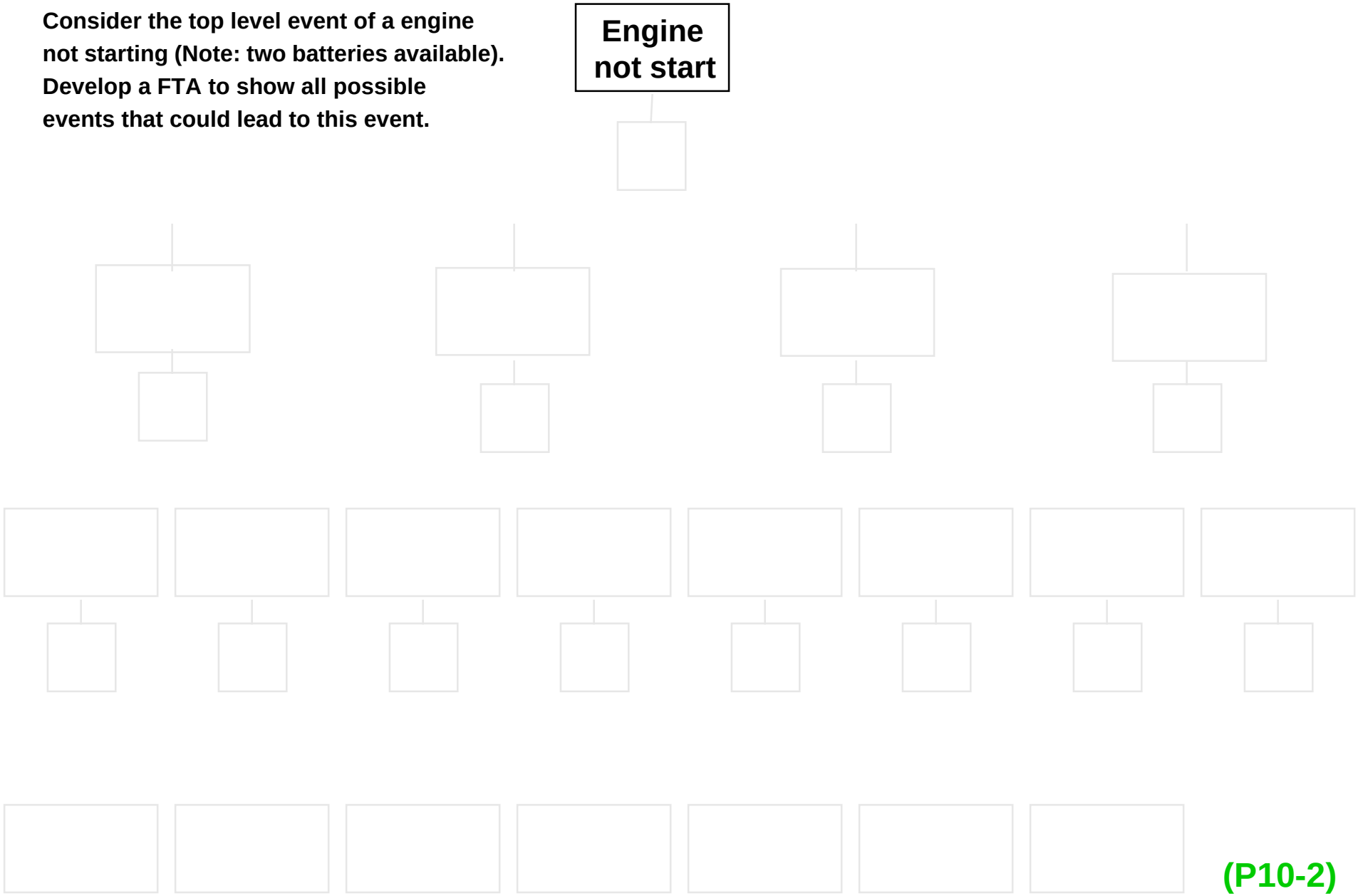
- **FTAs are used in safety critical systems especially where human life is involved. FTAs are also used to evaluate other potentially damaging events during test, build or operation.**
- **FTAs identify all the causes of a SINGLE failure mode.**
- **FTAs can be used in diagnostic work for a system failure.**
- **FTAs complement FMEAs keying in on the worst identified failure modes.**

END

F

FAULT TREE ANALYSIS of _ENGINE START_. by:___ Date __/__/__

Consider the top level event of a engine not starting (Note: two batteries available). Develop a FTA to show all possible events that could lead to this event.



F

FAULT TREE ANALYSIS of _____ by:___ Date __/__/__